INTRODUCTION

There is no such thing as perfect security. Advances in technology will always outpace our ability to effectively secure our networks from attackers. At Mandiant, we call this the "Security Gap." There is no technical or legislative solution that can eliminate this gap. Security breaches are inevitable because determined attackers will always find a way through the gap. This sounds disparaging, but it is not new information. Seasoned security professionals have been aware of the security gap throughout their careers.

While the problem is not going away any time soon, Mandiant saw companies make significant progress in their ability to Attack the Security Gap™ over the past year. In 2012, 37% of the organizations we responded to discovered the intrusion themselves, versus just 6% of the organizations we helped in 2011. We also saw more than a 40% improvement in the median time an attacker was present on a victim network — down to 243 days from 416 days in 2011. We note, however, that this downward shift in the median was accompanied by a higher mean days of compromise. In other words, more organizations are doing a better job of proactively identifying problems, but there are still outliers who are compromised for several years before they detect they are compromised.

In this M-Trends report, we present two different perspectives. First, a look at the tactics that the adversary is using to compromise organizations: the subversion of IT contractors, the extensive reconnaissance used by attackers, the persistent re-compromise of valuable targets, and strategic Web compromises. These four trends are about the business side of exploitation.

We also provide an attacker's perspective on a compromise with an overview of the APT1 threat actor, and a link to over 3,000 technical indicators that Mandiant is providing to the community.

Effectively attacking the security gap requires the best people, technology, and threat intelligence possible. It also requires collaboration and information sharing across our industry. It is our hope that the 2013 M-Trends and corresponding Web content can help your organization start to close this gap.